Securing Wireless Networks for PCI Compliance

Using Fortinet's Secure WLAN Solution to Meet Regulatory Requirements

Introduction

In the wake of many well-documented data breaches, standards such as the Payment Card Industry Data Security Standard (PCI DSS) have improved the overall security of data in retail networks. However, they are still seen as prime targets due to the sensitive nature of the data collected.

This paper is intended for CIOs and CISOs in the retail industry. Maintaining compliance with PCI DSS is a top concern as there are significant effects on business operations, payment card transactions, organizational security and data protection. In addition, the influx of wireless technology and the push for more customer engagement via mobile devices has made compliance with PCI DSS more challenging.

This paper will discuss how Fortinet secures traditional retail store data and how retailers can maintain compliance with PCI DSS while providing secure wireless networking at the same time.

The Impact of Wireless LANS (WLANs) in Retail Environments

Wireless networking has become an integral component of the retail industry in the past few years, driven primarily by the increase performance and ease of deployment of wireless networks. Also, with the adoption of smart phones and tablets, retailers want to monetize their wireless networks by increasing the engagement of consumers in or around their stores. In order to be competitive, retailers must address all of following new business requirements:

Allowing Secure Wireless LAN (WLAN) Access for Customers and Employees

As contradictory as it may have sounded only a few years ago, retailers are now looking for ways to *increase* the access customers have to applications and the Internet inside their stores. Additionally, many retailers are also encouraging increased interaction between employees and customers by employing tablets to help consumers browse for products, schedule appointments and even act as the Point of Sale (POS) terminal.

Examples of this new connected retail experience abound. One example is clothing manufacturer Guess? Inc. Guess allows customers in-store access to the wireless network and encourages interaction with social media for customers in the store. Many other retailers are looking to enhance the consumer experience through the interaction of in-store networks and applications.

The most obvious security concern with this approach is ensuring that payment information is kept separate and secured from other end-user data and general Internet traffic. This requires a variety of technologies including encryption, granular device- and user-based policy enforcement , wireless traffic management / traffic shaping technology to ensure that the payment network is accessible to only specific users and devices and that the data is always the top priority.

Increased Use of Analytics

Many retailers have also expanded their use of analytics to collect more data about consumers and their habits. This information is varied and can be considered highly personal. Information such as time spent shopping, what products the consumer looks at and eventually buys, and a variety of other

data can be collected by wireless networks and shared with the retailer.

Any analytics information collected by a retailer regarding consumers and their buying habits is regarded by most shoppers as confidential. While most regulations do not address the collection of analytics, some countries do have specific laws around privacy and the collection of data. Additionally, there are potential trust issues associated with the breach of any retail data, analytics included.

Constant Contact through Social Media and Mobile Applications

Since retailers are encouraging increased interaction with customers through social media and applications, the risks of a malicious third party spreading malware to unsuspecting consumers increases. Protecting in-store networks from malware and other application threats becomes the responsibility of the store if they encourage end users to connect through their wireless. An infection through an in-store wireless connection that steals data could become a public relations nightmare for a retailer.

All of these new requirements increases the complexity of the network and makes compliance with PCI DSS more difficult than ever before. Since most of these new technologies revolve around wireless networks, additional technology and security considerations must be in place in order to ensure compliance while maintaining a competitive edge.

Keeping Wireless Networks Compliant with PCI-DSS

With PCI DSS being the core regulatory requirement for retail networks, it is important to understand the standard and how PCI DSS defines sensitive information. The PCI DSS is a global security standard provided by the Payment Card Industry's Security Standards Council (PCI SSC) and requires certifiable support by any organization accepting credit and debit cards issued by the main brands such as Visa, MasterCard or American Express. It includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures for data. The impacts of cardholder data breaches are profound and PCI continues to modify the requirements to address the ever-changing threat landscape.

PCI DSS affects both wired and wireless networks; however wireless network present many additional challenges in regards to meeting the standard. One primary benefit of PCI DSS is that it has forced many retailers to consider all the various systems containing data they need to protect. Whether it is credit card repositories, detailed customer information, or the company's own intellectual property, PCI DSS requires an audit of systems and processes to determine how best to secure that data.

Table 1 illustrates some of the key PCI DSS objectives and the corresponding security requirement.

Table 1 - Key PCI Objectives and Requirements

CONTROL OBJECTIVE	REQUIREMENT
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all acccess to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Program	12. Maintain a policy that addresses Information Security

Key Challenges for Meeting PCI Compliance in Wireless Environments

Wireless networks present their own unique sets of challenges. When meeting compliance mandates like PCI DSS, retailers must remain cognizant about the differences between wired and wireless networks and take special care in segmenting and security the different types of networks that may be carrying cardholder data. Figure 1 illustrates the complex mix of devices that exist in the modern retail network. Some of the key challenges associated with maintaining PCI compliance in WLAN environments are listed below.

Logging all Wired and Wireless Traffic for Potential Attacks

PCI DSS mandates that periodic monitoring is needed to keep unauthorized or rogue wireless devices from compromising the security of the Cardholder Data Environment (CDE). That means all networks containing CDE must check for presence of rogue APs and take necessary measures. Unfortunately, intrusion detection in wireless LANs is more complicated than a wired LAN given lack of physical control over devices and the shared medium characteristics of wireless. Since separation of trusted and untrusted networks is critical in running a secure retail operation, it is imperative that the WLAN security technology can detect and disable unauthorized wireless devices connected to the CDE.

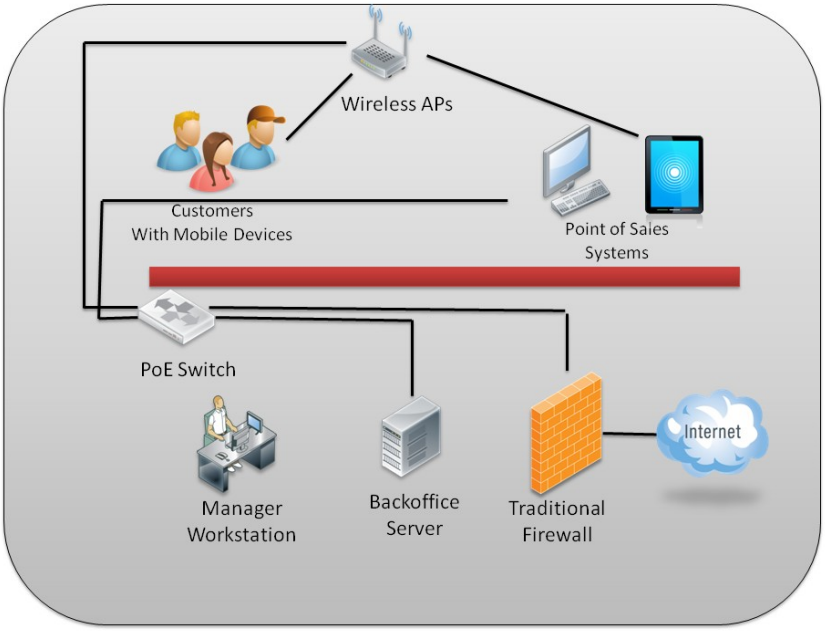

Figure 1 - The Modern Retail Network

Rogue access points may be introduced to the CDE through various means, including:

- Sniffing unprotected traffic outside the physical building using an access point
- Inserting a WLAN card into a file/application server, laptop, printer or other devices
- Attaching an unknown WLAN router to the network

Retailers need a sophisticated security platform to detect rogue access points and attacks from wherever they occur. This requires technology capable of analyzing attacks coming across both the wired and wireless network. There are two ways to accomplish this: configuring separate wired and wireless systems with identical policies, or using an integrated LAN/WLAN security system.

Ensuring Consistent Use of Strong Wireless Authentication and Encryption

PCI DSS mandates the use of strong wireless authentication and encryption to ensure that card data is transferred in an encrypted format. PCI DSS also requires that organizations avoid weak encryption standards such as WEP. The challenge for organizations is enforcing the selection of the appropriate authentication and encryption standards across the wired and wireless infrastructure. This requires equipment that not only supports a wide variety of options, but that can enforce the application of policy related to the appropriate encryption standard.

Developing and Enforcing Wireless Usage Policies Across the Entire Network

The PCI DSS mandates the need for acceptable usage policies and procedures, which include those for wireless devices. The importance here is that

organizations understand how wireless is to be used within their environment, how it is to be secured and deployed and how the organization will address incidents as they occur. Another important aspect the policy should address is how employees can and should use their authorized wireless devices. Just specifying a policy is not enough, technical controls must be in place that enforces wireless usage policy thereby preventing sensitive data loss.

Properly Segmenting Traffic on Wireless Networks

As long as WLAN traffic never touches cardholder data, then that WLAN is considered an out of scope network (one that does not have to adhere PCI DSS). However, if that WLAN is connected to a network that does process cardholder data, then according to PCI DSS, a firewall should separate and monitor that WLAN.

Given the current trend of providing increased access to end users on the retailer network, segmentation becomes particularly challenging. In order to ensure proper segmentation of the network and separation of the data the network must be able to identify data, applications, and traffic regardless of source.

Fortinet Provides a PCI DSS Compliance Platform

The wide range of security objectives retailers have to meet may seem daunting at first glance. Organizations that have attempted to solve the problem through point solutions often found their security incomplete and expensive.

There is a secure and affordable wireless solution to the PCI compliance challenge already at hand: Fortinet offers a centrally managed, unified solution at low cost of ownership that far surpasses competitive approaches (see Figure 2). Fortinet's approach is based on a purposeful architecture designed to provide best-in-class integrated wired and wireless solutions while meeting regulatory compliance (see Table 2) Some of the key features provided by Fortinet appliances are described below.

A Full Security Suite

Fortinet's Unified Threat Management (UTM) security platform FortiGate provides organizations the ability to protect any distributed network with the fastest security technology on the market. FortiGate appliances also give administrators the freedom to deploy the wide range of security technologies available, to fit any dynamic network environment.

By adopting Fortinet, retailers benefit from reduced complexity as well as full protection of technologies such as next generation firewalling, IPS, Data Loss Prevention (DLP), application control, and vulnerability management which have historically been offered to wired infrastructures only.

Device and Traffic Visibility and Logging

Providing secure wireless connectivity requires device agnostic policies to be in place. Retailers cannot predict all the devices that might enter the network as well as differentiate between employee owned and customer owned devices. Security policies need to be defined broadly.

Fortinet allows organizations to define granular policies based on device type (iPhone, iPad, Android devices, Laptops, etc.). By accurately detecting and securing all devices touching the network, as well as scanning for and suppressing rogue access points, Fortinet allows retailers to interact with customers with the latest technology tools while still adhering to

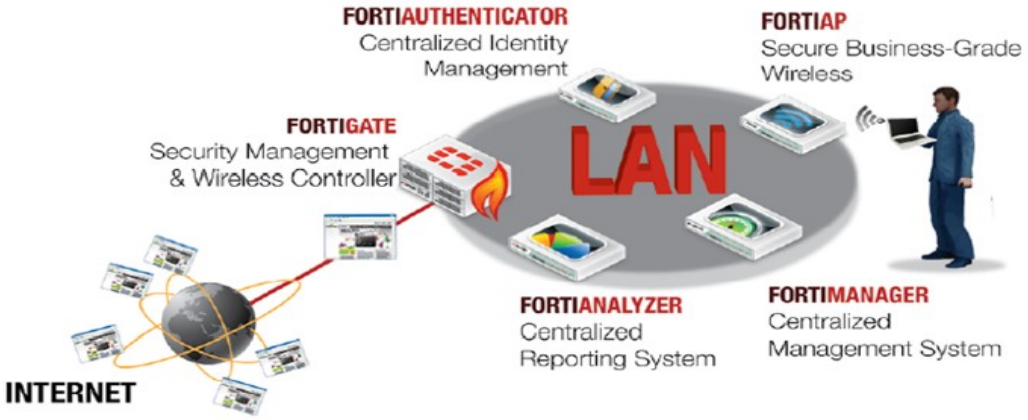

Figure 2 - Fortinet Provides a Complete Wired and Wireless Solution

CONTROL OBJECTIVE	REQUIREMENT	FORTINET SOLUTION
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data	**FortiGate** integrated firewall functionality
	2. Do not use vendor-supplied defaults for system passwords and other security parameters	**FortiDB** vulnerability assessment and auditing **FortiScan** OS vulnerability management **FortiWeb** web application firewall
Protect Cardholder Data	3. Protect stored cardholder data	**FortiDB** vulnerability assessment and auditing **FortiWeb** web application firewall
	4. Encrypt transmission of cardholder data across open, public networks	**FortiGate** IPSEC VPN
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware	**FortiGate** Integrated AV **FortiClient** Integrated AV **FortiMobile** Integrated AV **FortiMail** Integrated AV **FortiGuard** Automated AV updates
	6. Develop and maintain secure systems and applications	**FortiDB** vulnerability assessment, auditing, and monitoring **FortiWeb** web application firewall **FortiScan** OS vulnerability management **FortiAnalyzer** network vulnerability scanning
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know	**FortiDB** vulnerability assessment, auditing, and monitoring
	8. Assign a unique ID to each person with computer access	**FortiGate** integrated database or hooks to Active Directory
	9. Restrict physical access to cardholder data	**Fortinet Professional Servies** in partnership with FortiPartner VAR solutionS
Regularly Monitor and Test Networks	10. Track and monitor all acccess to network resources and cardholder data	**FortiDB** auditing and monitoring **FortiAnalyzer** event reporting, vulnerability scanning
	11. Regularly test security systems and processes	**FortiDB** vulnerability assessment **FortiScan** OS vulnerability management
Maintain an Information Security Program	12. Maintain a policy that addresses Information Security	**FortiManager** security policy management

Table 2 - PCI Objectives and Fortinet Solutions

the strict PCI DSS security guidelines.

End-to-End Security Policies and Controls

Fortinet allows retailers to provide a single policy across access points, security appliances and switched devices. This simplified the security process and ensures that no gaps exist in an organization's security controls.

Constant Threat Protection

Given the speed with which new attacks are released to the wild, it is imperative that retailers have protection in place to guard against the latest attacks. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms. With the FortiGuard Subscription Services enabled, customers can rest assured that their Fortinet security platforms are performing optimally and protecting their corporate assets with the latest security technology.

The FortiGuard security team continually develops new attack filters to address the latest vulnerabilities and incorporates these filters into security signatures. Signatures are created not only to address specific exploits, but also potential attack permutations, protecting customers from zero-day threats. Fortinet deploys a variety of security filters for a variety of products including traffic anomaly filters, vulnerability-based filters, and signatures.

Signatures are delivered to customers on a regular basis with no user interaction required. This constant updating against both the most prevalent and unexploited threats provide significant protection to Fortinet customers.

By providing every facet of the infrastructure – from wireless APs, to the wireless controller, to POE switches, Fortinet provides an end-to-end, wired and wireless infrastructure that shares the same set of security policies – guaranteeing complete and consistent enforcement across the entire organization.

Integrated, Centralized Authentication

Integrated, centralized authentication with single sign-on and policy enforcement is critical to providing secure access to the appropriate systems that compromise a retail environment. Administrators may be responsible for systems extending out from the core of the network to

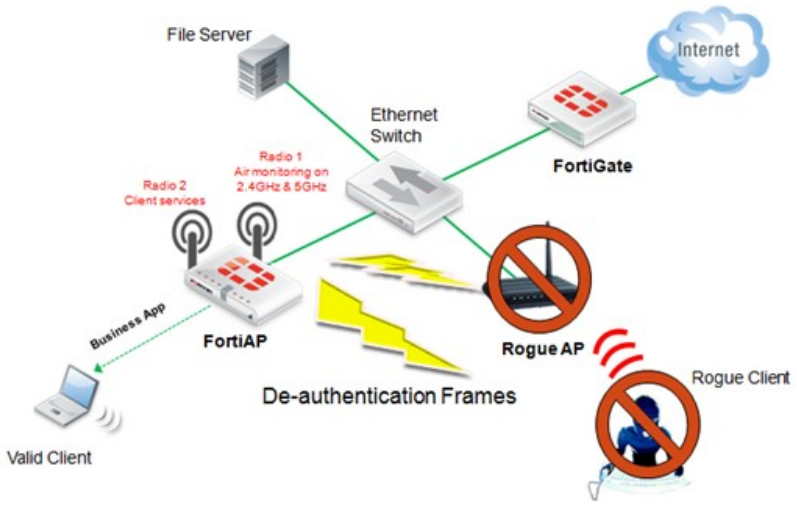

Figure 3 - Rogue AP Detection and Suppression Using FortiGate and FortiAP Devices

thousands of braches, and need consistent, secure access to those systems.

Even at branch locations, employees and devices will need access to a wide variety of corporate, back-end systems. FortiAuthenticator provides a secure system that tightly integrates with existing directory systems and allows for the quick deployment of seamless identity and access control.

Integrated Wireless Controllers Reduce Cost and Complexity.

Fortinet gives organizations an extensive range of wireless devices to choose from in order to ensure that they can deploy the architecture that makes sense for their organization. A variety of thick and thin APs allow for extensive customization of the wireless network. However, the most important aspect of Fortinet's wireless solution is the integrated wireless controller.

Every FortiGate has an integrated wireless controller and comes ready to manage APs out of the box. This tight coupling of security and wireless in unique in the industry and provides the core differentiator between Fortinet and its competitors. All UTM functions can be applied on wireless traffic – giving end users the unique ability to quickly scan applications and data on the wireless network.

Additionally, rogue AP detection and suppression capabilities are also configured on the FortiGate – providing a truly centralized location for providing the organization's security policies (see Figure 3).

Conclusion

Modern retailers are faced with the daunting task of having to add new technology to their networks in order to remain competitive while keeping sensitive data flowing through those networks secure. PCI DSS is the foundation of security in the retail space and requires a wide variety of mitigating controls be in place to protect cardholder data against accidental or intentional loss.

Fortinet's consolidated approach to security controls through Universal Threat Management (UTM) and Intrusion Prevention Systems (IPS) in every WLAN controller allows for the consolidation of policies on both wired and wireless networks. Fortinet WLAN solutions are business grade wireless platforms that provide automatic PCI DSS compliance so that retailers can focus on business at hand.

GLOBAL HEADQUARTERS
Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia
Antipolis, France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480